	L #	Search Text	DBs	Time Stamp	Hits
1	L1	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:11	582
2	L2	713/175.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:11	324
3	L3	713/156.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:11	684

	L #	Search Text	DBs	Time Stamp	Hits
4	L4	709/224.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:11	5004
5	L5	709/225.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:11	2333
6	L6	380/277.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:12	1046

	L #	Search Text	DBs	Time Stamp	Hits
7	L7	380/278.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:12	400
8	L8	ibm.asn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:12	48844
9	L9	yeager.in. and william.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:13	187

	L #	Search Text	DBs	Time Stamp	Hits
10	L10	pabla.in. and kuldip.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:13	2
11	L11	L9 and L10	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:13	1
12	L12	L11 and L8	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:13	0

	L #	Search Text	DBs	Time Stamp	Hits
13	L13	peer same session	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:14	2165
14	L14	peer same (session adj3 (key or cipher))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:14	143
15	L15	L14 and (generat$3 with (public or asymmetric) near5 (key or cipher))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:15	38

	L #	Search Text	DBs	Time Stamp	Hits
16	L16	L14 and (generat$3 with "from public key")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:15	0
17	L17	(session or traffic) near (key) near (peer)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:16	13
18	L18	L15 and L17	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:16	3

	L #	Search Text	DBs	Time Stamp	Hits
19	L19	(peer-to-peer) near (session or traffic) near (key) near (encrypt$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:16	0
20	L20	(generat$3) near (session or traffic) near (key) near (public) near (key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:17	21
21	L21	L15 and L20	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2006/06/22 17:17	1

Terms used
peer to peer session key public key Diffie Hellman shared key nodes

Found **394** of **178,880**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 On the performance of group key agreement protocols

Yair Amir, Yongdae Kim, Cristina Nita-Rotaru, Gene Tsudik

August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3

Publisher: ACM Press

Full text available: pdf(469.07 KB) Additional Information: full citation, abstract, references, index terms

Group key agreement is a fundamental building block for secure peer group communication systems. Several group key management techniques were proposed in the last decade, all assuming the existence of an underlying group communication infrastructure to provide reliable and ordered message delivery as well as group membership information. Despite analysis, implementation, and deployment of some of these techniques, the actual costs associated with group key management have been poorly understood ...

Keywords: Group Communication, Group Key Management, Peer Groups, Secure Communication

2 Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

3 Public-key support for group collaboration

Carl Ellison, Steve Dohrmann
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(561.61 KB) Additional Information: full citation, abstract, references, index terms

This paper characterizes the security of group collaboration as being a product not merely of cryptographic algorithms and coding practices, but also of the man-machine process of group creation. We show that traditional security mechanisms do not properly address the needs of a secured collaboration and present a research prototype, called NGC (next generation collaboration), that was designed to meet those needs. NGC distinguishes itself in the care with which the man-machine process was analy ...

Keywords: Human-computer interface, IPsec, PGP, PKI, S/MIME, SDSI, SPKI, SSH

4 A key-chain-based keying scheme for many-to-many secure group communication

Dijiang Huang, Deep Medhi
November 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 4
Publisher: ACM Press
Full text available: pdf(311.81 KB) Additional Information: full citation, abstract, references, index terms

We propose a novel secure group keying scheme using *hash chain* for *many-to-many* secure group communication. This scheme requires a *key predistribution center* to generate multiple hash chains and allocates exactly one hash value from each chain to a group member. A group member can use its allocated hash values (secrets) to generate group and subgroup keys. Key distribution can be offline or online via the key distribution protocol. Once keys are distributed, this scheme enab ...

Keywords: Hash chain, key chain, many-to-many secure group communication, secure group communication

5 Security: Fast authenticated key establishment protocols for self-organizing sensor networks

Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, Jinyun Zhang
September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications**
Publisher: ACM Press
Full text available: pdf(303.05 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we consider efficient authenticated key establishment protocols between a sensor and a security manager in a self-organizing sensor network. We propose a hybrid authenticated key establishment scheme, which exploits the difference in capabilities between security managers and sensors, and put the cryptographic burden where the resources are less constrained. The hybrid scheme reduces the high cost public-key operations at the sensor side and replaces them with efficient symmetric- ...

Keywords: elliptic curve cryptography, key establishment, security, sensor network

6 The LOCKSS peer-to-peer digital preservation system

Petros Maniatis, Mema Roussopoulos, T. J. Giuli, David S. H. Rosenthal, Mary Baker
February 2005 **ACM Transactions on Computer Systems (TOCS)**, Volume 23 Issue 1
Publisher: ACM Press

Full text available: pdf(715.30 KB) Additional Information: full citation, abstract, references, index terms

The LOCKSS project has developed and deployed in a world-wide test a peer-to-peer system for preserving access to journals and other archival information published on the Web. It consists of a large number of independent, low-cost, persistent Web caches that cooperate to detect and repair damage to their content by voting in "opinion polls." Based on this experience, we present a design for and simulations of a novel protocol for voting in systems of this kind. It incorporates rate l ...

Keywords: Rate limiting, digital preservation, replicated storage

7 Sensor networks: Random key-assignment for secure Wireless Sensor Networks

Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei

October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks**

Publisher: ACM Press

Full text available: pdf(162.10 KB) Additional Information: full citation, abstract, references, citings

A distributed Wireless Sensor Network (WSN) is a collection of *n* sensors with limited hardware resources. Sensors can exchange messages via Radio Frequency (RF), whose range usually covers only a limited number of other sensors. An interesting problem is how to implement secure pair-wise communications among any pair of sensors in a WSN. A WSN requires completely distributed solutions which are particularly challenging due to the limited resources and the size of the network. Moreover, WS ...

Keywords: distributed wireless sensors networks, key management protocols, secure pair-wise communications, sensor-to-sensor authentication

8 Best poster papers from MobiHoc 2002: Virtual operator based AAA in wireless LAN hot spots with ad-hoc networking support

Junbiao Zhang, Jun Li, Stephen Weinstein, Nan Tu

June 2002 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 6 Issue 3

Publisher: ACM Press

Full text available: pdf(180.11 KB) Additional Information: full citation, abstract, references, citings, index terms

Sound and effective authentication, authorization and accounting (AAA) schemes for convenient and secure mobile wireless accesses are of great importance given the increased popularity and business opportunities in public wireless LAN hot spots. One possible scheme, which uses the mobile users' service providers as the single point of contact for all AAA transactions, is emerging as a very promising solution. We refer to such service providers as "virtual operators". In this paper, we discuss va ...

9 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler

September 2002 **Wireless Networks**, Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA

provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

10 Cryptography as an operating system service: A case study

Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside
February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

11 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(118.52 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

12 Key management: Fully self-organized peer-to-peer key management for mobile ad hoc networks

Johann van der Merwe, Dawoud Dawoud, Stephen McDonald
September 2005 **Proceedings of the 4th ACM workshop on Wireless security WiSe '05**
Publisher: ACM Press
Full text available: pdf(237.33 KB) Additional Information: full citation, abstract, references, index terms

Mobile ad hoc networks (MANETs) offer communication over a shared wireless channel without any pre-existing infrastructure. Forming peer-to-peer security associations in MANETs is more challenging than in conventional networks due to the lack of central authority. The main contribution of this paper is a low complexity key management scheme that is suitable for fully self-organized MANETs. The proposed peer-to-peer key management scheme uses subordinate public keys and crypto-based identifiers t ...

Keywords: Mobile IPv6, crypto-based identifiers, identity-based cryptography, mobile ad hoc networks, network level key distribution, network security, pairwise key management, peer-to-peer key management, self-organization, subordinate public keys

13 Just fast keying: Key agreement in a hostile internet

William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available: pdf(324.39 KB) Additional Information: full citation, abstract, references, index terms

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of tradeoffs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

14 Improving key predistribution with deployment knowledge in static sensor networks

Donggang Liu, Peng Ning

November 2005 **ACM Transactions on Sensor Networks (TOSN)**, Volume 1 Issue 2

Publisher: ACM Press

Full text available: pdf(639.52 KB) Additional Information: full citation, abstract, references, index terms

Pairwise key establishment is a fundamental security service for sensor networks. However, establishing pairwise keys in sensor networks is a challenging problem, particularly due to the resource constraints on sensor nodes and the threat of node compromises. This article proposes to use both *predeployment and postdeployment knowledge* to improve pairwise key predistribution in static sensor networks. By exploiting the predeployment knowledge, this article first develops two key predistrib ...

Keywords: Sensor networks, key management, key predistribution

15 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings

16 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to

accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

17 Exploring adaptability of secure group communication using formal prototyping techniques

Sebastian Gutierrez-Nolasco, Nalini Venkatasubramanian, Mark-Oliver Stehr, Carolyn Talcott
October 2004 **Proceedings of the 3rd workshop on Adaptive and reflective middleware ARM '04**
Publisher: ACM Press
Full text available: pdf(276.83 KB) Additional Information: full citation, abstract, references

Traditionally, adaptability in communication frameworks has been restricted to predefined choices without taking into consideration tradeoffs between them and the application requirements. Furthermore, different applications with an entire spectrum of requirements will have to adapt to these predefined choices instead of tailoring the communication framework to fit their needs. In this paper we extend an executable specification of a state-of-the-art secure group communication subsystem to ex ...

18 DHT: OpenDHT: a public DHT service and its uses

Sean Rhea, Brighten Godfrey, Brad Karp, John Kubiatowicz, Sylvia Ratnasamy, Scott Shenker, Ion Stoica, Harlan Yu
August 2005 **Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '05**
Publisher: ACM Press
Full text available: pdf(535.74 KB) Additional Information: full citation, abstract, references, index terms

Large-scale distributed systems are hard to deploy, and distributed hash tables (DHTs) are no exception. To lower the barriers facing DHT-based applications, we have created a public DHT service called OpenDHT. Designing a DHT that can be widely shared, both among mutually untrusting clients and among a variety of applications, poses two distinct challenges. First, there must be adequate control over storage allocation so that greedy or malicious clients do not use more than their fair share. Se ...

Keywords: distributed hash table, peer-to-peer, resource allocation

19 Routing & performance modelling: A novel solution for achieving anonymity in wireless ad hoc networks

Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba
October 2004 **Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks**
Publisher: ACM Press
Full text available: pdf(219.31 KB) Additional Information: full citation, abstract, references, index terms

A mobile ad hoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a wireless and mobile ad hoc network usually seek the help of other intermediate nodes to establish communication channels. In such an open environment, malicious intermediate nodes can be a threat to the security and/or anonymity of the exchanged data between the mobile nodes. While data encryption can protect the content exchanged between nodes, routing information may reveal va ...

Keywords: ad hoc, network simulator ns-2, routing, security, wireless networks

20 Applications, services, and architecture: Reputation-based Wi-Fi deployment protocols and security analysis

Naouel Ben Salem, Jean-Pierre Hubaux, Markus Jakobsson

October 2004 **Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots**

Publisher: ACM Press

Full text available: pdf(395.70 KB) Additional Information: full citation, abstract, references, index terms

In recent years, wireless Internet service providers (WISPs) have established thousands of WiFi hot spots in cafes, hotels and airports in order to offer to travelling Internet users access to email, web or other Internet service. However, two major problems still slow down the deployment of this kind of networks: the lack of a seamless roaming scheme and the variable quality of service experienced by the users. This paper provides a response to these two problems: We present a solution that, ...

Keywords: QoS, WiFi networks, billing, protocols, reputation systems, roaming, security

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Results for "((peer-to-peer<in>metadata) <and> (session key, public key<in>metadata))<..." e-mail
Your search matched 1 of 1360403 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

((peer-to-peer<in>metadata) <and> (session key, public key<in>metadata))<and> Search

Check to search only within this results set

» Key

Display Format: Citation Citation & Abstract

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Key agreement in peer-to-peer wireless networks**
Cagalj, M.; Capkun, S.; Hubaux, J.-P.;
Proceedings of the IEEE
Volume 94, Issue 2, Feb. 2006 Page(s):467 - 478
Digital Object Identifier 10.1109/JPROC.2005.862475
AbstractPlus | Full Text: PDF(464 KB) IEEE JNL
Rights and Permissions